الرئاسة العامة لشؤون المسجد الحرام والمسجد النبوي

مركز تقنية المعلومات

#التقنية_في_خدمتكم

رؤية VISION 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

كيف نكون قدوة؟



يقظ

للتوعية بأمن المعلومات

حملة توعويّة للتعريف بأهمية أمن المعلومات في الرئاسة العامة لشؤون المسجد الحرام والمسجد النبوي

قسم أمن المعلومات الإلكتروني

الرئاسة العامة لشؤون المسجد الحرام والمسجد النبوي

مركز تقنية المعلومات

#التقنية_في_خدمتكم









حملة توعويَّة للتعريف بأهمية أمن المعلومات في الرئاسة العامة لشؤون المسجد الحرام والمسجد النبوي

قسم أمن المعلومات الإلكتروني



مقدمة

تشكل معلوماتك الشخصية وجهاز الحاسب الخاص بك صيدا ثمينا للمخترقين وغيرهم من الفضوليين الذين يعملون على الانترنت . وقد أظهرت الإحصاءات أن البشر هم الحلقة الأضعف في تأمين المعلومات.

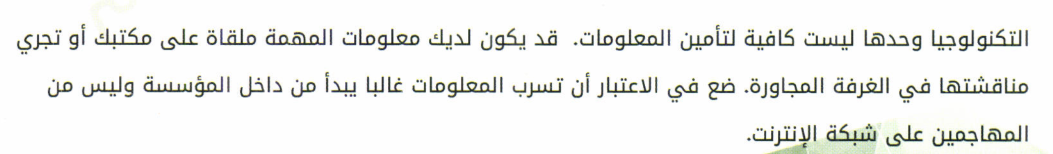
لذلك سيحاول مخترقو الإنترنت الإيقاع بك لاتخاذ الإجراءات التي من شأنها أن تفتح أمامهم الأبواب. فهم يستهدفونك من أجل :



- الوصول إلى معلومات مالية أو غيرها من المعلومات المهمة.
- استخدام جهاز الحاسب الخاص بك لمهاجمة أنظمة حاسوبية أخرى .
- سرقة هويتك .
- الإضرار بسمعتك .
- اكتساب ميزة تنافسية عن طريق سرقة الأبحاث .

التكنولوجيا وحدها ليست كافية لتأمين المعلومات. قد يكون لديك معلومات المهمة ملقاة على مكتبك أو تجري مناقشتها في الغرفة المجاورة. ضع في الاعتبار أن تسرب المعلومات غالبا يبدأ من داخل المؤسسة وليس من المهاجمين على شبكة الإنترنت.

اتبع مبادئ توجيهية بسيطة بديهية، وسوف تساعدك على إبقاء جميع المعلومات التي لديك آمنة.



كلمات المرور: مفاتيح مملكتك

- اجعل كلمة المرور كإبرة في كومة قش يصعب على القراصنة العثور عليها. اتبع هذه الإرشادات عند استخدام كلمات المرور الخاصة بك.



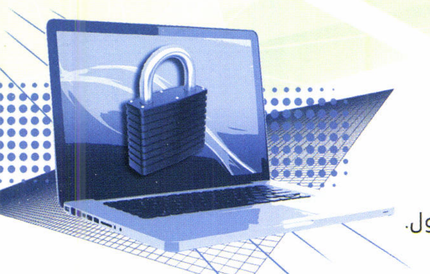
- لا تستخدم كلمات المرور التي يسهل تخمينها.
- استخدم كلمات مرور صعبة وسهلة التذكر.
- كلمات المرور الصعبة تحتوي حروف كبيرة وصغيرة بالإضافة إلى الأرقام والرموز.
- لا تشارك أحداً في كلمة المرور الخاصة بك.
- لا تستخدم كلمة المرور نفسها للعمل والحسابات الشخصية.
- لا تكتب كلمة المرور الخاصة بك وتتركها حيث يمكن للآخرين العثور عليها.
- لا تستخدم جهاز حاسب آلي عام لتسجيل الدخول إلى مواقع ذات معلومات المهمة .





تصفح آمن للإنترنت

- قم بتحديث متصفح الإنترنت باستمرار.
- احرص على عدم حفظ كلمات المرور من خلال برامج المتصفح ، لأنه يمكن للمخترقين الحصول عليها عند اختراق الجهاز.
- احرص على مسح المحفوظات والملفات المؤقتة والكوكيز من برنامج المتصفح بشكل مستمر، خاصة بعد زيارة المواقع الحساسة مثل البنوك.
- اضبط إعدادات المتصفح لتحديد المواقع التي يُسمح لها باستخدام الكوكيز.
- امنع النوافذ المنبثقة، فبعضها ربما يشكل هجمات خبيثة أو خفية.
- لا تحاول التخلص من النوافذ المنبثقة عند ظهورها بالضغط على زر "موافق" بل أغلقها فوراً.
- تأكد من ضبط إعدادات الأمان والخصوصية والمحتوى لمتصفح الإنترنت. يجب أن يكون مستوى الأمان "متوسط" على أقل تقدير.
- قم بتعطيل مكونات ActiveX و Java و JavaScript في حال رغبتك بتصفح مواقع غير موثوق بها.



أمن الحاسوب المحمول

- احذر ترك كلمة المرور أو أرقام سرية في حقيبة الحاسوب المحمول.
- اجعل حاسوبك المحمول دائما معك ولا تتركه بعيدا عنك.
- شفر بياناتك المخزنة على الحاسوب المحمول باستخدام برامج التشفير.
- استخدم الأدوات الخاصة بحماية الحواسيب المحمولة مثل الكيبل المعدني الذي يستخدم لتثبيت الحاسوب المحمول في كرسي ثقيل أو منضدة أو مكتب.
- لا تترك جهازك في الفندق أو لدى مكتب الاستقبال.
- لا تترك الحاسب المحمول في السيارة.
- تأكد من عدم انتهاء صلاحية برامج الحماية, أما إذا كانت منتهية فعليك تجديدها أو استبدالها فورا.
- حدّث برامج مكافحة الفيروسات والبرامج المضادة للتجسس وكذلك برامج جدار الحماية قبل استخدام حاسوبك المحمول.
- أغلق خاصية الاتصال اللاسلكي (Wi-Fi) في حاسوبك عند عدم الحاجة لاستخدامها فذلك يساعد على منع المخترقين من الدخول إلى حاسوبك المحمول بطريقة لاسلكية.
- استخدم حاجبا للشاشة لمنع الآخرين من التلصص عليها أثناء تعاملك مع معلومات حساسة في مكان عام.



أمن هاتفك المحمول

- تأكد من تفعيل طلب رقم التعريف الشخصي (الرقم السري للشريحة PIN) لهاتفك الجوال.
- قم بوضع كلمة سرية على لوحة مفاتيح الجوال بحيث لا يمكن لأحد استخدامه حال غيابك.
- لا تُمكن أي شخص غير موثوق فيه من استخدام هاتفك الجوال.
- تأكد من وضع هاتفك الجوال في مكان آمن حماية له من السرقة.
- يوجد العديد من برامج مكافحة الفيروسات الخاصة بالهاتف الجوال التي يمكنك استخدامها.
- لا تستقبل أي رسائل بواسطة البلوتوث من أشخاص لا تعرفهم ، وقم بتعطيل خاصية قبول الاتصال تلقائياً ، و قم بإغلاق خدمة البلوتوث عند عدم الحاجة إليها.
- عند صيانة هاتفك الجوال ابحث عن وكلاء الصيانة المعتمدين واحذر من محلات الصيانة المنتشرة غير المعتمدة.
- تجنب قدر الإمكان تخزين الصور الحساسة في هاتفك الجوال.
- عند الرغبة في ببيع هاتفك الجوال تأكد من حذف جميع البيانات المخزنة عليه ، أو على بطاقة الذاكرة ، ومن ثم إعادة ملئها ببيانات أخرى غير حساسة ، أو قم باستخدام إحدى برامج طمس البيانات .
- في حال وجودك في اجتماع هام أو سري قم بإغلاق هاتفك الجوال وإخراج البطارية منه احترازاً من وجود برامج تجسس لها القدرة على تشغيل الجهاز بدون علم المستخدم والتصنت عليه.
- شفر البيانات الموجودة على هاتفك الجوال لحمايتها في حال السرقة.

أمّن نفسك ضد الإصطياد الإلكتروني

- لاتفتح الروابط أو مرفقات البريد الإلكتروني المشبوهة أو التي من أشخاص مجهولين أو التي لا يتوقع وصولها من الطرف الآخر.
- يجب عليك التأكد من تحديث أنظمة التشغيل والتطبيقات بشكل دوري وفعال، وذلك تجنباً لاستغلال الثغرات الحديثة لإصابة الأنظمة والأجهزة بالبرامج الخبيثة.
- استخدم برامج مكافحة الفيروسات والتأكد من تحديثها دوريا واستخدم أنظمة الكشف المتطورة عن البرمجيات الخبيثة APT. ومتابعة التدقيق في سجلات برامج مكافحة الفيروسات لكشف أي علامات على الإصابة ببرامج خبيثة.
- خذ نسخ احتياطية للمعلومات والملفات المهمة بشكل دوري مناسب ويجب أن تكون في مكان غير جهازك.
- احذر من الذين يتصلون لطلب معلومات شخصية دون سابق معرفة.
- لا تكشف عن بياناتك الشخصية مثل رقم الهوية أو أرقام الحسابات أو كلمات المرور عبر الهاتف أو البريد الالكتروني أو غيرها من وسائل الاتصال الالكترونية إلا إذا تأكدت من أن الجهة المطالبة بتلك البيانات جهة موثوقة.
- اقرأ بعناية كافة تعليمات الخصوصية والأمن في المواقع التي تتعامل معها.
- إذا اتصل بك أحد وقال لك بأن معلوماتك قد تم اختراقها فلا تزوده بأي معلومة وإنما اتصل بالجهة المعنية لإرشادك.
- راجع كشوفاتك البنكية بشكل دوري لتتأكد من عدم وجود عمليات مشبوهة.
- لا ترسل أي معلومات مالية إلا بعد تشفيرها, من خلال المواقع التي تبدأ ب(https).

البريد الإلكتروني



- إذا تلقيت رسالة بريد إلكتروني تطلب منك النقر على رابط أو إرسال معلومات شخصية عن طريق البريد الإلكتروني، فهذه على الأرجح محاولة خادعة تهدف إلى الحصول على معلومات شخصية ويسمى هذا النوع من الهجوم (تصيد).
- إذا كان البريد الإلكتروني المرسَل يبدو غريبا أو مختلفا عن النمط العام، فإنه على الأرجح محاولة خبيثة للوصول إلى المعلومات الخاصة بك وبحساباتك.
- لا تضغط على الروابط التي تتلقاها في رسائل البريد الإلكتروني إلا إذا كنت متأكدا تماما من أنها آمنة.
- لا تستجب لرسائل البريد الإلكتروني أو المكالمات الهاتفية التي تطلب معلومات شخصية أو سرية قبل التحقق من هوية الطالب وغرضه من ذلك .
- لا ترسل معلومات سرية عن العمل عن طريق البريد الإلكتروني الخارجي مثل Gmail أو! Yahoo .

نصائح أمنية عامة

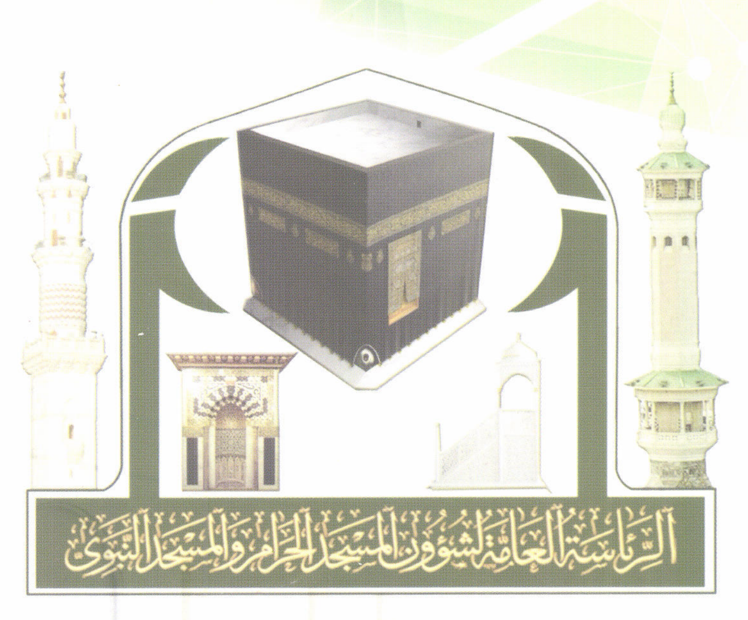


- بلّغ عن الحوادث الأمنية لمركز تقنية المعلومات مباشرة.
- تقيَّد بالسياسات الأمنية لمركز تقنية المعلومات.
- أمّن مكان عملك.
- استخدم برامج التشفير لأجهزتك المحمولة المختلفة.
- أمّن جهازك الشخصي قبل ترك مقعدك.
- اختر كلمة مرور قوية يصعب تخمينها.
- لا تخبر أحداً بكلمة مرورك.
- لا تكشف عن أي معلومات شخصية أو سرية ما لم يكن ذلك ضروريا للغاية وإلى الطرف المناسب.
- لا تترك معلومات حساسة متناثرة في مكان عملك.
- لا تثبت تطبيقات غير مصرح بها أو غير مرخصة.
- تأكد دائما أن برامج مكافحة البرامج الضارة مثبتة بنظام التشغيل.

اتصل بنا

- إذا كنت غير متأكد من أنه تم تثبيت برامج مكافحة البرامج الضارة في جهاز الكمبيوتر الخاص بك في العمل وأنها تعمل بشكل صحيح.
- إذا كنت تعتقد أن معلومات حساسة تعرضت للتسريب.
- إذا كنت غير متأكد من سلامة رسالة تلقيتها.
- إذا كنت تعتقد أنه تم انتهاك خصوصية جهاز الكمبيوتر الخاص بك أو اختراقه.
- إذا تلقيت رسالة جيدة الصياغة من أي شخص في الرئاسة تطلب منك معلومات شخصية بما في ذلك كلمات مرور حسابك والحسابات المصرفية وما إلى ذلك.
- إذا كان لديك أسئلة أخرى تتعلق بحماية المعلومات.
- يسعدنا تواصلك معنا عن طريق إرسال رسالة إلكترونية على البريد الإلكتروني **security@gph.gov.sa**





#التقنية_في_خدمتكم

قسم أمن المعلومات الإلكتروني

تنفيذ
إدارة المطبوعات والنشر
PUB@GPH.GOV.SA